Alle praktijkgerichte artikels hebben we gebundeld in de rubriek 'Doe het zelf'. Vragen? Opmerkingen? Tips? Stuur ze naar Clickx Brieven, Minoc Business Press, Everdongenlaan 15 bus 1, 2300 Turnhout. Je kan ook faxen naar 014/44.20.66 of mailen naar brieven.clickx@minoc.com.

IN DIT NUMMER

MOEILIJK? MAKKELIJK?

In de 'Doe het zelf'-rubriek vind je zowel bijdragen voor beginners als voor mensen die al aardig overweg kunnen met hun computer. We hebben een systeem bedacht waarmee je in één oogopslag kan zien hoe moeilijk of makkelijk een artikel is. Zo weet je meteen of het een makkie wordt of dat je er toch even al je concentratie voor nodig hebt...

★☆☆ VOOR BEGINNERS

★★☆ VOOR IEDEREEN

★★★ VOOR GEVORDERDEN

Brief van de week

De Clickx-redactie wordt elke dag overstelpt met vragen van lezers. Sommige problemen zijn te specifiek om in het magazine te behandelen, maar andere vragen zijn dan weer zo interessant dat ze meer verdienen dan een kort antwoordje. Daarom selecteren we vanaf nu voor elke Clickx Magazine een vraag van een lezer, die we dan uitwerken in een complete workshop. De vraag vind je op deze pagina, de workshop staat op de volgende twee pagina's. Veel plezier!

Spionnenjacht



Sinds kort krijg ik regelmatig de volgende tekst op mijn scherm te zien: "Your computer is infected! Windows has detected spyware infection! [...] Click here to protect your computer from spyware!" Wat is er aan de hand?

PALMER NIJS

Computergebruikers zijn als de duivel voor virussen, Trojanen, hackers, wormen en spionnen... De angst voor malware zit er dus flink ingebakken, en niet helemaal onterecht! Maar tegelijk spelen allerlei onverlaten hier handig op in, bijvoorbeeld door je tijdens het surfen pop-ups te tonen die je op een gevaarlijke systeeminfectie wijzen. Gelukkig bieden ze ook de 'remedie': een druk op de OK-knop volstaat om je pc te desinfecteren... Dat had je gedacht... precies dáárdoor haal je pas malware binnen! Palmer is op een gelijkaardige manier in de val gelopen: in de workshop die je op de twee volgende pagina's terugvindt, vertellen we je wat er precies aan de hand is en – belangrijker nog – hoe je allerlei vormen van spyware buiten houdt!





Eerst het vingertje, dan kassa kassa!

De onheilspellende boodschap die Palmer geregeld ziet opduiken, is op zich de voorbode van een infectie door Spyhoax-A, alias Troj_Dloader. SQ. Hij heeft het wellicht binnengehaald via een of andere download of door zijn browser op een bepaalde webstek af te stemmen. Terwijl je dit bericht ziet verschijnen, sprokkelt het onding nog een reeks bijkomende bestanden binnen die hij standaard naar de map **C:\Program Files\SpySheriff** kopieert. Hiermee haal je een spionnenjager binnen die je om de haverklap op nieuwe onheilsboodschappen trakteert – tot wanneer je de betaalversie van Spy Sheriff downloadt. Spy Sheriff maakt echter gebruik van handige trucjes om je deze meldingen te blijven geven, ook als je de tool verwijdert.

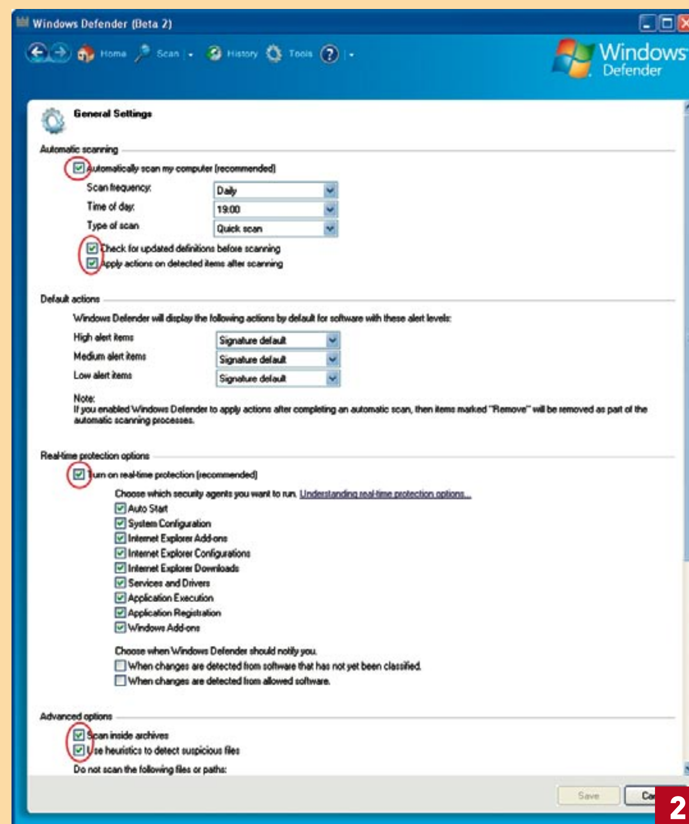
Ons advies: zorg dat je altijd de nieuwste updates voor Windows XP en voor je browser binnenhaalt (via de Windows Update-site), en laat je niet om de tuin leiden door dubieuze meldingen. En natuurlijk installeer je een betrouwbare (!) spionnenjager die je braafjes up-to-date houdt. Bekende gratis exemplaren zijn alvast Ad-Aware SE Personal **www.lavasoftusa.com/software/adaware** en Spybot Search & Destroy **www.safer-networking.org/nl/index.htm**. Ook Microsoft heeft al een tijdje zijn AntiSpyware-tool in de running, en onlangs is daar het meer geavanceerde Windows Defender voor in de plaats gekomen. Die zit momenteel in een stabiele bèta 2-fase, en je kan hem gratis downloaden. De tool zal trouwens een vast onderdeel vormen van Windows Vista. We vertellen je hoe je die optimaal inzet in je strijd tegen de spionnen...

STAP 1 / INSTALLATIE

De thuishaven van Windows Defender is **www.microsoft.com/athome/security/spyware/software**. Via een opvallende knop kan je de tool hier downloaden. De download maakt wel gebruik van de dienst 'genuine Microsoft Windows'. Anders gezegd: wie niet over een geldige Windows-licentie beschikt, valt buiten de prijzen. Om deze controle toe te laten, zal je wel eerst nog een ActiveX-component moeten accepteren. Als alles in orde is, kan je doorgaan via de knop **Download** (6,4 MB). Het betreft een msi-bestand, dat je activeert door erop te dubbelklikken. Een installatiewizard staat je bij, zodat je weinig meer hoeft te doen dan op **Next** te klikken. Wel moet je halverwege te kennen geven of je wil meewerken aan de SpyNet online community. Ga je hierop in, dan worden je scanresultaten en ook je reacties daarop richting internet gestuurd. Als beloning krijg jij dan ook te zien hoe anderen bij vergelijkbare detecties reageerden. Een venster verder moet je nog kiezen tussen een **Complete** of een **Custom** installatie: selecteer hier bij voorkeur de eerste optie. Even later rond je de procedure af met de **Install**-knop.

STAP 2 / BASISCONFIGURATIE

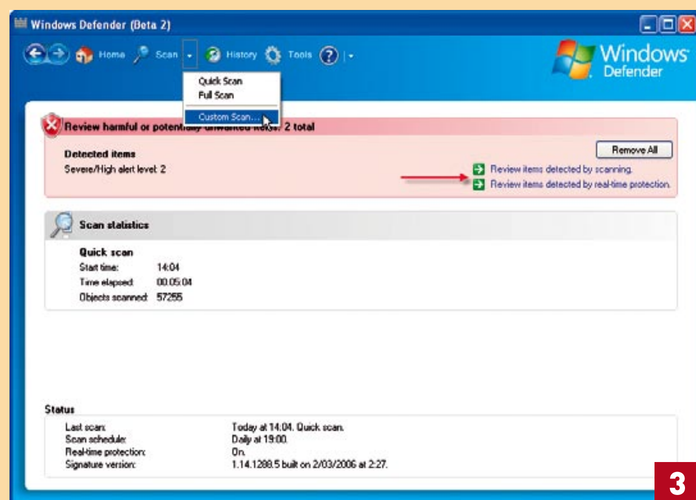
Meteen na de installatie stelt de tool voor om online naar updates te zoeken en tegelijk een snelle scanronde te activeren. Geen slecht idee, als je het ons vraagt – hoewel je beide acties ook later nog op elk moment kan uitvoeren. Laten we eerst eens kijken hoe je Windows Defender naar je hand zet. Om de module te openen, kan je ofwel met de rechtermuisknop op het bijhorende icoontje in de systeembalk klikken en **Open** kiezen, ofwel via **Start**, **Alle Programma's**, **Windows Defender** selecteren. Dé knop om je voorkeuren kenbaar te maken, is **Tools**. Hier klik je in eerste instantie **General Settings** aan. Er verschijnt een nieuw venster met een indrukwekkend aantal opties, waarvan de meeste zichzelf uitwijzen. We raden je aan de standaardinstellingen (zie de rode indicaties op afbeelding 2) ongemoeid te laten. Die zorgen er namelijk voor dat Windows Defender allerlei real-time beveiligingen activeert (zoals een bescherming tegen invoegtoepassingen en tegen dubieuze programma's die automatisch samen met Windows willen opstarten), en dat je systeem op gezette tijden automatisch gescand wordt. Wel kan je het tijdstip van deze scanrondes aanpassen: standaard staat dat ingesteld op 2 uur 's nachts. Bevestig eventuele wijzingen met de knop **Save**.



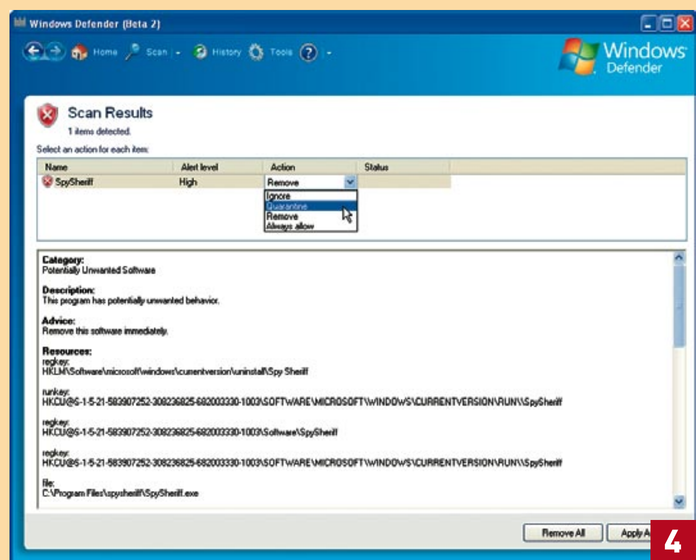
Gelukkig zijn de standaardinstellingen goed te pruimen.

STAP 3 / SCANRONDE

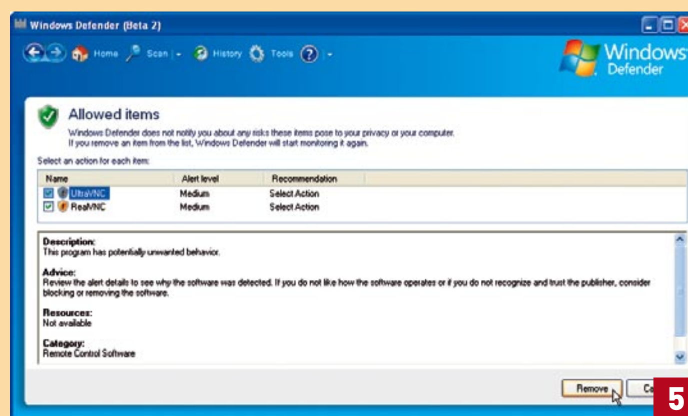
Er valt heus nog wel wat te sleutelen aan Windows Defender, maar laten we eerst ons systeem eens grondig door de roskam halen. Daarvoor dient de **Scan**-knop, bovenaan de module. Wat en hoe grondig je precies wil scannen, bepaal je via het witte pijltje, naast de **Scan**-knop. Je hebt de keuze uit drie opties. Terwijl een **Quick Scan** zich beperkt tot de meest gebruikelijke infectiehaarden, worden bij een **Full Scan** zowat alle bestanden en toepassingen van je systeem doorgelicht. Het spreekt voor zich dat deze laatste variant heel wat arbeidsintensiever is. De derde optie, **Custom Scan**, is vooral interessant als je de scanronde wil beperken tot bepaalde bestandsmappen – bijvoorbeeld als je pas nieuwe bestanden op je schijf gezet hebt (zie afbeelding 3). In dat geval kan je via de knop **Select** de gewenste stations of mappen selecteren, waarna je bevestigt met **OK** en vervolgens met **Scan Now** – hoewel Windows Defender tijdens onze tests hardnekkig méér dan alleen maar de geselecteerde mappen onderzocht... Overigens laat een controle zich op elk moment onderbreken via de knop **Stop Scanning**.



Een scanronde laat zich beperken tot specifieke mappen.



Alert level high: niet meteen het voordeel van de twijfel!



Dan toch maar de versnipperaar in?

STAP 4 / REACTIE

Na afloop toont Windows Defender je (via de knop **Home**) keurig een rapport met de scanresultaten. Heb je prijs, dan is het natuurlijk verleidelijk meteen de knop **Remove All** in te drukken, zodat je meteen van de boosdoeners verlost bent. Je doet er echter verstandiger aan eerst langs de links **Review items** [...] te lopen. Die geven je namelijk meer detailinformatie over de vermeende spion, én je leest meteen af waar die zich zoal in je systeem verstopt heeft. Het is ook altijd verstandig om zo'n rapport af te drukken. Hier kan je eveneens aanduiden wat je precies met dit verdachte sujet wil doen: definitief verwijderen (**Remove**), dit keer ongemoeid laten (**Ignore**), voor eeuwig en altijd je fiat geven (**Always Allow**) of naar een veilig, afgeschermd plekje verbannen (**Quarantine**) (zie afbeelding 4). Met **Apply Actions** voer je de ingestelde actie uit.

STAP 5 / HET VOORDEEL VAN DE TWIJFEL

Het zal wel duidelijk zijn dat de zuiverste actie een definitieve verwijdering is. Maar het kan natuurlijk ook gebeuren dat je de toepassing voorlopig het voordeel van de twijfel wil geven. In dat geval kies je wellicht best voor een van de drie andere acties. Maar wat als achteraf blijkt dat je je toch vergist hebt, en het wel degelijk om een spion blijkt te gaan? Geen man overboord: het volstaat dan even de knop **History** of **Tools** aan te klikken. In beide vensters tref je namelijk links aan waarmee je specifieke onderdelen weer uit de lijst van (tijdelijk) toegelaten of in quarantaine geplaatste bestanden kan halen. Klik je **Quarantined items** aan, dan kan je het bewuste item aanstippen, waarna je kiest tussen **Restore** (de toepassing wordt weer toegelaten) en **Remove** (het programma wordt definitief uitgeschakeld). Klik je **Allowed items** aan, dan kan je op een vergelijkbare manier geselecteerde items met de knop **Remove** definitief naar de eeuwige jachtvelden sturen (zie afbeelding 5). Clickx wenst je alvast een spionnenvrije computer toe! ♦

VAKTAAL | A - M | N - Z

ACTIVEX: Ontwikkeld door Microsoft. Dankzij ActiveX kunnen websites en programma's (automatisch) bepaalde code opstarten en uitvoeren. Deze code is meestal heel compact en kan verschillende functies bevatten.